DATA SHEET

FortiWeb™
Web Application Firewall

FortiWeb

FortiWeb 400C, 1000D, 3000D/3000DFsx and 4000D

Web Application Firewall

Web Application Firewall — Secures web applications to help customers meet compliance requirements

Web Vulnerability Scanner — Scans, analyzes and detects web application vulnerabilities

Application Delivery — Assures availability and accelerates performance of critical web applications

Emerging Threats Create New Challenges

The continued evolution of the threat landscape has enabled individuals and groups to launch orchestrated attacks on organizations' infrastructure for criminal or political gain. Attackers now use a wealth of methods to infect hosts and control compromised systems through organized botnets for automated phishing, spamming, and DDoS attacks. DoS attacks are morphing from traditional network layer attacks to sophisticated layer seven attacks targeting application resources rather than bandwidth, flying under the radar of traditional DoS mitigation tools. Organizations now need new tools to protect against these emerging threats and the more traditional hacking methods such as SQL Injection and Cross-site-scripting.

Unmatched Protection for Web Applications

The FortiWeb family of web application firewalls provides specialized, layered application threat protection for medium and large enterprises, application service providers, and SaaS providers. FortiWeb web application firewall protects your web-based applications and Internet-facing data from attack and data loss. Using advanced techniques to provide bidirectional protection against malicious sources and sophisticated threats like SQL injection and Cross-site scripting, FortiWeb platforms help you prevent identity theft, financial fraud and corporate espionage. FortiWeb delivers the technology you need to monitor and enforce government regulations, industry best practices, and internal policies.

Unmatched Protection for Web Applications

- ICSA WAF certified
- WAF and integrated scanner aid in PCI 6.6 compliance
- Network and Application layer DoS protection
- Ongoing and automated protection against botnets and malicious sources
- Bot dashboard helps analyzing traffic from malicious robots, crawlers, scanners and search engines
- User behavior and web application structure analysis
- Geo IP analytics and security
- Antivirus file scanning
- Protection against the OWASP Top 10
- Periodic updates from FortiGuard® Labs

Accelerate Deployment and Lower Costs

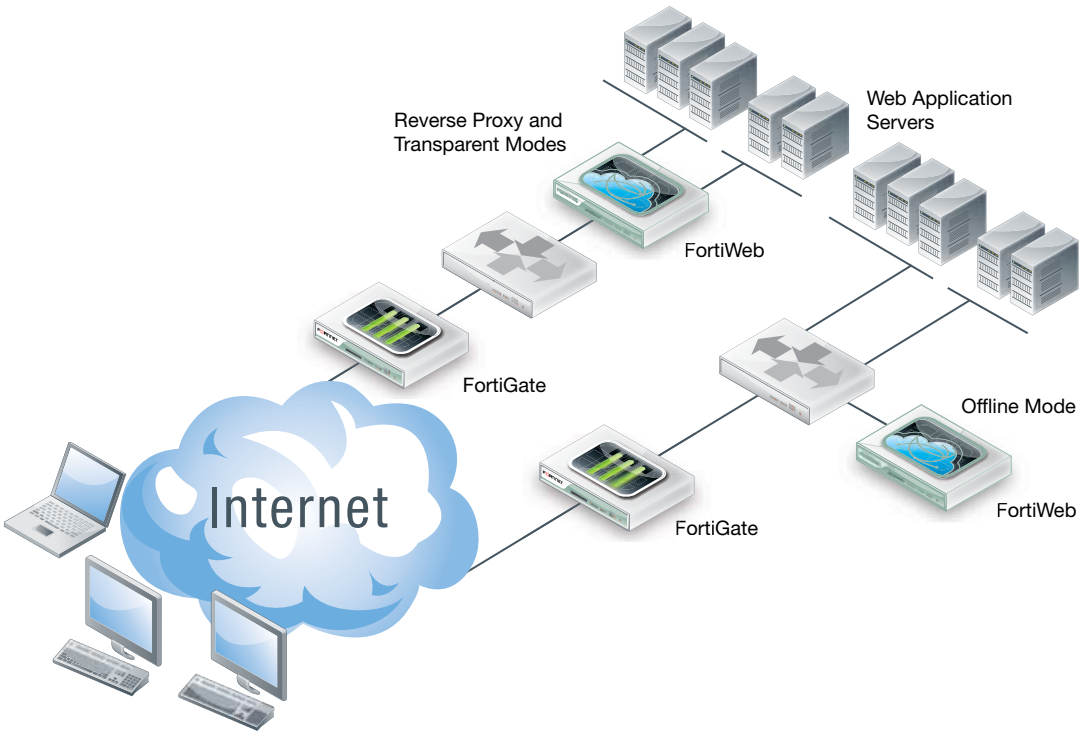
FortiWeb significantly reduces deployment costs by consolidating Web Application Firewall, web traffic acceleration, and application traffic balancing into a single device with no per-user pricing. It drastically reduces the time required to protect your regulated Internet-facing data and eases the challenges associated with policy enforcement and regulatory compliance. Its intelligent, application-aware load balancing and data compression and optimization engine increases application performance, improves resource utilization and application stability while reducing server response times.

Geo IP Analytics and Security

FortiWeb's real time data analysis provides an analytic interface that helps organizations analyze their web application usage from multiple vectors, maps requests to their geographic location and allows blocking access from specific countries.

DEPLOYMENT

- Reverse Proxy – Provides additional capabilities such as URL rewrite and advanced routing capabilities.
- Inline Transparent – Layer two bridge that does not require network level redesign.
- True Transparent Proxy – Layer two deployment with no need for network level redesign. The traffic is internally terminated to provide more functionality than pure inspection.
- Offline Sniffing – Monitors environments with zero network footprint and latency.



HIGHLIGHTS

Enhanced Protection with IP Reputation Service

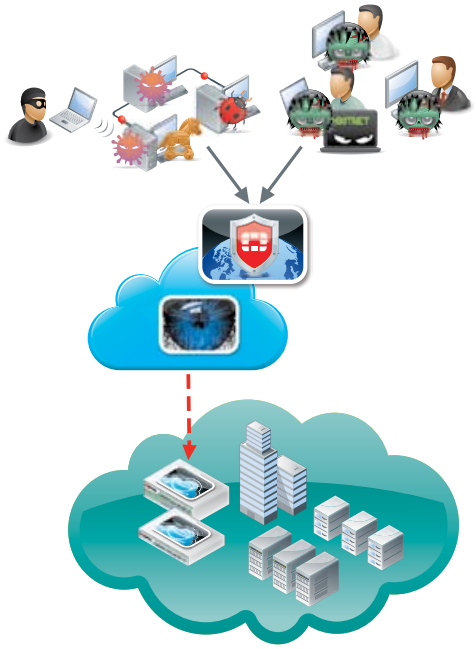
As the internet evolves hackers have begun using orchestrated attacks on organizations' infrastructure. Attackers now use a wealth of methods to infect innocent hosts, and control these infections through organized botnets in order to launch automated phishing, spamming, and DDoS attacks.

The FortiGuard IP Reputation Service for FortiWeb platforms aggregates data from locations and sources around the world that collaborate to provide up to date information about threatening sources. With feeds from distributed network gateways combined with world class research done from FortiGuard Labs, organizations can stay up to date and proactively block attacks.

Protect your organization from multiple attack vectors

FortiGuard's IP Reputation Service categorizes and blocks threats from sources associated with:

- DDoS: Sources identified taking part of DDoS attacks
- Phishing: Sources identified taking part of Phishing attacks or hosting Phishing web sites
- Anonymous Proxies: anonymized traffic arriving from paid or anonymous proxies used to disguise real client identity
- Malicious Sources: hosts known to be infected with malicious software
- Spammers: hosts known to send spam



Ultimate Protection and Monitoring

- **Auto-Learn Security Profiling**
  Automatically and dynamically build a security model of protected applications by continuously monitoring realtime user activity. Eliminate the need for manual configuration of security profiles.
- **Application Layer Vulnerability Protection**
  Provide out of the box protection for the most complex attacks such as SQL Injection, Cross Site Scripting, CSRF and many others. Together with the Auto Learn profiling system and advanced abilities, FortiWeb is able to create rules down to the single application element.
- **DoS Protection**
  Multiple protection policies for network and application layer denial of service threats. Sophisticated mechanism helps identify and block automated attacks.
- **Data Leak Prevention**
  Extended monitoring and protection for credit card leakage and application information disclosure by tightly monitoring all outbound traffic. Allow customers to create their own granular signatures and DLP patterns together with predefined rules for any type of events.
- **Site Publishing and SSO**
  Publish Microsoft applications such as Outlook Web Access and SharePoint with authentication delegation and single sign on integration.
- **Web Defacement Protection**
  Unique capabilities for monitoring protected applications for any defacement and ability to automatically and quickly revert to stored version.
- **Correlated Threat Detection**
  Advanced correlation of multiple attack detection mechanisms uncover sophisticated threats. Through integration of elements such as attack signatures, suspicious URLs and unknown headers, multi-event thresholds can be set up to increase attack accuracy and minimize false positive detections.
- **Vulnerability Assessments**
  Automatically scans and analyzes the protected web applications and detects security weaknesses, potential application known and unknown vulnerabilities to complete a comprehensive solution for PCI DSS.
- **HTTP RFC Compliance Validation**
  FortiWeb blocks any attacks manipulating the HTTP protocol by maintaining strict RFC standards to prevent attacks such as encoding attacks, buffer overflows and other application specific attacks.
- **Antivirus**
  Scan file uploads using Fortinet's Antivirus engine with regular FortiGuard updates.

HIGHLIGHTS

Flexible Deployment and Efficient Management

- **Multiple Deployment Options**
  Transparent Inspection and True Transparent Proxy, Reverse Proxy and Offline modes allow deploying FortiWeb into any environment.
- **Geo IP and Bot Analysis**
  Map requests to their geographic location and analyze traffic from malicious robots, crawlers, scanners, website scrapers, and search engines.
- **IPv6 Ready**
  Simplify network configuration with dual-stack support for both IPv4 to IPv6 and IPv6 to IPv4 communication.
- **Authentication Offload**
  Offload your web server authentication to the FortiWeb platform while supporting different authentication schemes such as Local, LDAP, NTLM, Kerberos and RADIUS with 2-factor authentication for RADIUS and RSA SecureID.
- **Pre-defined Policies**
  Allows for one click deployments and greatly eases the process of policy creation.
- **High Availability**
  The high availability mode provides configuration synchronization and allows for a network-level failover in the event of unexpected outage events. Integrated bypass interfaces provide additional fail open capability for single box deployments.
- **Centralized Logging and Reporting**
  Centrally manage all logs and reports from multiple FortiWeb gateways with FortiAnalyzer integration.
- **Administrative Domains**
  Provide role-based administration rights to designated domain owners to manage their own applications separately from others on the same FortiWeb device.
- **Centralized Management**
  Configure and manage multiple FortiWeb gateways from a single FortiWeb console (requires additional license).
- **Virtualization**
  Provides a Virtual Appliance for VMware ESX/ESXi, Microsoft Hyper-V, Citrix XenServer, Open Source Xen, and Amazon AWS platforms. AWS supports pre-purchased FortiWeb VM licenses or can be directly purchased through the AWS Marketplace.

Application Delivery

- **Application Aware Load Balancing**
  Intelligent, application aware layer 7 load balancing eliminates performance bottlenecks, reduces deployment complexity and provides seamless application integration.
- **Data Compression**
  Allows efficient bandwidth utilization and response time to users by compressing data retrieved from servers.
- **SSL Offload**
  With the integration of award winning FortiASIC™ technology, FortiWeb is able to process tens of thousands of web transactions by providing hardware accelerated SSL offloading.

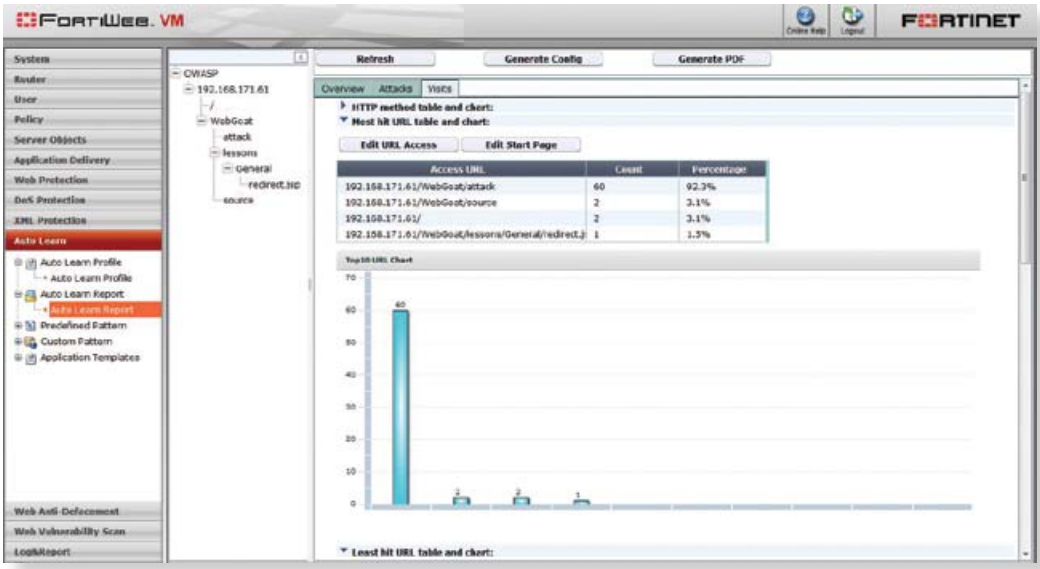
Aids in Compliance

- **PCI DSS Compliance**
  FortiWeb is the only product that provides a Vulnerability Scanner module within the web application firewall that completes a comprehensive solution for PCI DSS requirement 6.6.
- **Protects Against OWASP Top 10**
  Incorporating a positive and a negative security module based on bidirectional traffic analysis and an embedded behavioral based anomaly detection engine FortiWeb fully protects against the OWASP TOP 10.
- **FortiGuard Labs**
  Utilizing Fortinet's renowned FortiGuard service, FortiWeb customers get up to date dynamic protection from the Fortinet Global Security Research Team, which researches and develops protection against known and potential application security threats.

HIGHLIGHTS

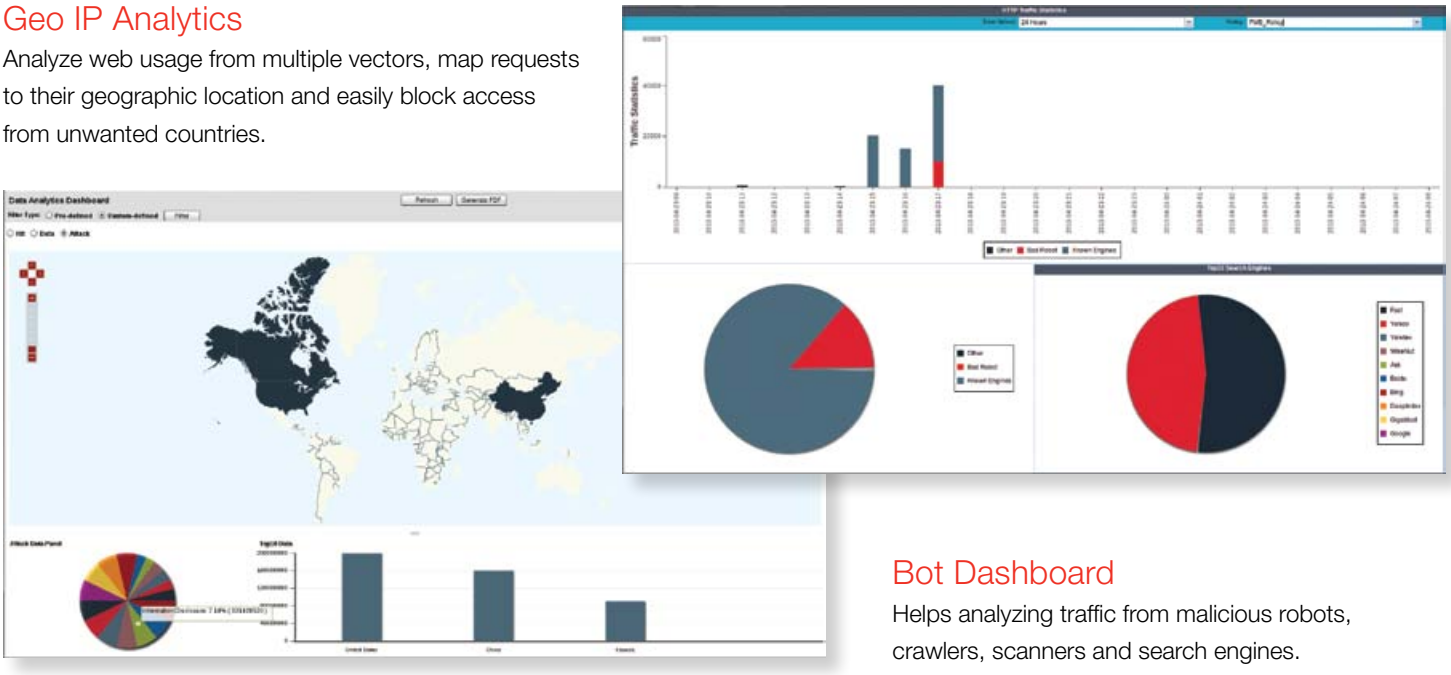
Application Profiling

The Auto-Learn profiling capability is completely transparent and does not require any changes to the application or network architecture. FortiWeb does not scan the application in order to build the profile, but rather analyzes the traffic as it monitors it flowing to the application. By creating a comprehensive security model of the application, FortiWeb can now protect against any known or unknown vulnerabilities or zero day attacks.



Geo IP Analytics

Analyze web usage from multiple vectors, map requests to their geographic location and easily block access from unwanted countries.



Analyze user geographic location and web site access based on Hit, Data and Attack vectors.

Bot Dashboard

Helps analyzing traffic from malicious robots, crawlers, scanners and search engines.

FortiWeb Protects Against a Wide Range of Attacks

- Cross Site Scripting
- SQL Injection
- Session Hijacking
- Cookie Tampering / Poisoning
- Cross Site Request Forgery
- Command injection
- Remote File Inclusion
- Forms Tampering
- Hidden Field Manipulation
- Outbound Data Leakage
- HTTP Request Smuggling
- Remote File Inclusion
- Encoding Attacks
- Broken Access Control
- Forceful Browsing
- Directory Traversal
- Site Reconnaissance
- Search Engine Hacking
- Brute Force Login
- Access Rate Control
- Schema Poisoning
- XML Intrusion Prevention
- Recursive Payload
- External Entity Attack
- Buffer Overflows
- Denial of Service
- Zero Day Attacks

SPECIFICATIONS

	FORTIWEB 400C	FORTIWEB 1000D	FORTIWEB 3000D/3000DFsx	FORTIWEB 4000D
Hardware				
10/100/1000 Interfaces (RJ-45 ports)	4	6 (4 bypass) 2x SFP GbE (non-bypass)	3000D: 6 and 2 bypass 3000DFsx: 6	8 (2 bypass)
1000Base-SX Bypass Interfaces	0	0	0	2
10G BASE-SR SFP+ Bypass interfaces	0	0	3000D: 0 3000DFsx: 2	2
USB Interfaces	1	2	4	4
Storage	1 TB	2x 2 TB	2x 2 TB	2x 2 TB
Form Factor	1U	2U	2U	2U
Power Supply	Standard	2U Hot Swap Redundant	2U Hot Swap Redundant	2U Hot Swap Redundant
System Performance				
Throughput	100 Mbps	750 Mbps	1.5 Gbps	4 Gbps
Latency	Sub-ms	Sub-ms	Sub-ms	Sub-ms
High Availability	Active/Passive	Active/Passive	Active/Passive	Active/Passive
Application Licenses	Unlimited	Unlimited	Unlimited	Unlimited
Administrative Domains	32	64	64	64
All performance values are "up to" and vary depending on the system configuration.				
Dimensions				
Height x Width x Length (inches)	1.7 x 17.1 x 14.3	3.50 x 17.24 x 14.49	3.44 x 20.0 x 29.72	3.44 x 20.0 x 29.72
Height x Width x Length (mm)	44 x 435 x 364	88 x 438 x 368	87.3 x 482 x 755	87.3 x 482 x 755
Weight	14.15 lbs (6.42 kg)	27.6 lbs (12.5 kg)	63 lbs (28.6 kg)	63 lbs (28.6 kg)
Rack Mountable	Yes	Yes, with flanges	Yes	Yes
Environment				
Power Required	100–240 VAC, 50–60 Hz, 4.0 Amp max	100–240 VAC, 50–60 Hz	100–240 VAC, 50–60 Hz	100–240 VAC, 50–60 Hz
Maximum Current	120V/4A, 240V/2A	100V/5A, 240V/3A	110V/10A, 220V/5A	110V/10A, 220V/5A
Power Consumption (Average)	100.3 W	115 W	393.6 W	393.6 W
Heat Dissipation	410.7 BTU/h	471 BTU/h	1,804.95 BTU/h	2,061.87 BTU/h
Operating Temperature	32–104°F (0–40°C)	32–104°F (0–40°C)	50–95°F (10–35°C)	50–95°F (10–35°C)
Storage Temperature	-13–158°F (-25–70°C)	-13–158°F (-25–70°C)	-40–149°F (-40–65°C)	-40–149°F (-40–65°C)
Humidity	10–90% non-condensing	5–95% non-condensing	20–90% non-condensing	20–90% non-condensing
Compliance				
Safety Certifications	FCC Class A Part 15, C-Tick, VCCI, CE, UL/cUL, CB	FCC Class A Part 15, UL/CB/cUL, C-Tick, VCCI, CE	FCC Class A Part 15, UL/CB/cUL, C-Tick, VCCI, CE	FCC Class A Part 15, UL/CB/cUL, C-Tick, VCCI, CE

	FORTIWEB-VM (1 vCPU)	FORTIWEB-VM (2 vCPU)	FORTIWEB-VM (4 vCPU)	FORTIWEB-VM (8 vCPU)
Hardware Specifications				
HTTP Throughput	25 Mbps	100 Mbps	500 Mbps	1 Gbps
Maximum HTTP transactions per second	3,000	8,000	24,000	36,000
Application Licenses	Unlimited	Unlimited	Unlimited	Unlimited
Administrative Domains	4 to 64 based on the amount of memory allocated			
Virtual Machine				
Hypervisor Support	VMware ESX / ESXi 4.0 / 4.1 / 5.0 / 5.1 / 5.5, Microsoft Hyper-V, Citrix XenServer 6.2, Open Source Xen 4.2, Amazon Web Services (AWS)			
vCPU Support (Minimum / Maximum)	1	2	2 / 4	2 / 8
Network Interface Support (Minimum / Maximum)	1 / 4 (10 VMware ESX)	1 / 4 (10 VMware ESX)	1 / 4 (10 VMware ESX)	1 / 4 (10 VMware ESX)
Storage Support (Minimum / Maximum)	40 GB / 2 TB	40 GB / 2 TB	40 GB / 2 TB	40 GB / 2 TB
Memory Support (Minimum / Maximum)	1,024 MB / Unlimited for 64-bit	1,024 MB / Unlimited for 64-bit	1,024 MB / Unlimited for 64-bit	1,024 MB / Unlimited for 64-bit
High Availability Support	Yes	Yes	Yes	Yes

Actual performance values may vary depending on the network traffic and system configuration. Performance metrics were observed using a Dell PowerEdge R710 server (2 x Intel Xeon E5504 2.0 GHz 4 MB Cache) running VMware ESXi 4.1 with 3 GB of vRAM assigned to the 4 vCPU and 8 vCPU FortiWeb Virtual Appliance and 1 GB of vRAM assigned to the 2 vCPU FortiWeb Virtual Appliance.

ORDER INFORMATION

Product	SKU	Description
FortiWeb 400C	FWB-400C-BDL	FortiWeb-400C Hardware plus 1 year 8x5 FortiCare and FortiGuard Bundle.*
FortiWeb 1000D	FWB-1000D-E07S-BDL	FortiWeb-1000D Hardware plus 1 year 8x5 FortiCare and FortiGuard Bundle.*
FortiWeb 3000D	FWB-3000D-E02S-BDL	FortiWeb-3000D Hardware plus 1 year 8x5 FortiCare and FortiGuard Bundle.*
FortiWeb 3000DFsx	FWB-3000DFSX-E02S-BDL	FortiWeb-3000DFsx Hardware plus 1 year 8x5 FortiCare and FortiGuard Bundle.*
FortiWeb 4000D	FWB-4000D-BDL	FortiWeb-4000D Hardware plus 1 year 8x5 FortiCare and FortiGuard Bundle.*
FortiWeb-VM01	FWB-VM01	FortiWeb-VM, up to 1 vCPU supported. 64-bit OS.
FortiWeb-VM02	FWB-VM02	FortiWeb-VM, up to 2 vCPUs supported. 64-bit OS.
FortiWeb-VM04	FWB-VM04	FortiWeb-VM, up to 4 vCPUs supported. 64-bit OS.
FortiWeb-VM08	FWB-VM08	FortiWeb-VM, up to 8 vCPUs supported. 64-bit OS.
Central Manager 10	FWB-CM-LIC-10	FortiWeb Central Manager license key, manage up to 10 FortiWeb devices.
Central Manager Unlimited	FWB-CM-LIC-UL	FortiWeb Central Manager license key, manage unlimited number of FortiWeb devices.

* The FortiGuard bundle includes the FortiWeb Security Service, FortiGuard IP Reputation Service and the FortiWeb Antivirus Service.

GLOBAL HEADQUARTERS
Fortinet Inc.
899 Kifer Road
Sunnyvale, CA 94086
United States
Tel: +1.408.235.7700
www.fortinet.com/sales

EMEA SALES OFFICE
120 rue Albert Caquot
06560, Sophia Antipolis,
France
Tel: +33.4.8987.0510

APAC SALES OFFICE
300 Beach Road 20-01
The Concourse
Singapore 199555
Tel: +65.6513.3730

LATIN AMERICA SALES OFFICE
Prol. Paseo de la Reforma 115 Int. 702
Col. Lomas de Santa Fe,
C.P. 01219
Del. Alvaro Obregón
México D.F.
Tel: 011-52-(55) 5524-8480